REMARKS

Claims 2-20 are pending in this application. Claim 1 is cancelled herein, and the dependent claims are correspondingly amended.

In accordance with 37 CFR 1.116(b), after a final rejection or other final action in an application, amendments may be made canceling claims. The applicant respectfully maintains that this amendment adds no new matter, and does not require an additional search, because claim 2, which is rewritten herein in independent form, including all of the limitations of cancelled claim 1, has been fully examined and specifically addressed in the final Office action, at page 4, lines 7-11.

The Office action rejects claims 1-20 under 35 U.S.C. 102(b) over Heys et al., "On The Design of Secure Block Ciphers", May 1994, hereinafter Heys. The applicant respectfully traverses this rejection.

The Office action provided a text-only copy of Heys, which did not include figures and equations. Attached is a complete copy of Heys.

Claim 2, upon which each of claims 3-12 depend, claims a method for cryptographically converting an input data block into an output data block that includes selecting a select permutation from a predetermined set of at least two permutations, wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.

As the title of Heys' article indicates, Heys addresses the selection of a permutation for use in a substitution box during the design of a block cipher. Heys presents criteria for such a selection to provide a secure block cipher to replace DES (Heys, Section I, first paragraph). Heys defines the desired properties (S1-S3, D1-D3) in Section III, and proposes the use of S-boxes that have good diffusion characteristics and small XOR pair probabilities in Section IV. S-boxes with good diffusion characteristics are generated, from which the preferred S-boxes (highly nonlinear and low XOR pair probability) are selected (Section IV, third paragraph).

Heys does not teach forming pairs of S-boxes wherein a weakness of one S-box is offset by a strength of another S-box. Heys does not acknowledge weaknesses associated with the selected S-boxes, and thus cannot be said to form a set of S-box permutations such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set, as specifically claimed by the applicant.

Because Heys does not teach forming sets of S-box permutations wherein a weakness of one permutation is offset by a strength of another permutation, as specifically claimed by the applicant, the applicant respectfully requests the Examiner's reconsideration of the rejection of claims 2-12 under 35 U.S.C. 102(b) over Heys.

Claim 13 claims a system for cryptographically converting an input data block into an output data block that includes a storage for storing a predetermined set of at least two permutations associated with an S-box, and a processor that is configured to, each time before using the S-box, randomly select a permutation from the set.

Heys does not teach randomly selecting a permutation from a stored set of permutations each time before using the S-box to convert an input data block into an output data block. Heys teaches randomly selecting S-box permutations that meet certain criteria during the design of a secure block cipher. The configuration of the selected S-boxes is as shown in Heys' Figure 1. Heys does not teach that each of these S-boxes includes at least two permutations, and does not teach selecting one of the at least two permutations each time before using the S-box, as specifically claimed in claim 13.

Because Heys does not teach storing at least two permutations in an S-box, and selecting one of the permutations each time before using the S-box, as specifically claimed in claim 13, the applicant respectfully requests the Examiner's reconsideration of the rejection of claim 13 under 35 U.S.C. 102(b) over Heys.

Claim 14, upon which claims 15-20 depend, claims a cryptographic encoder that includes a plurality of substitution boxes, wherein each of the substitution boxes is configured to receive a control signal and a set of data bits, and substitutes a first output

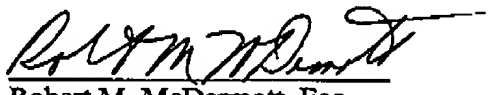
value for the set of data bits if the control signal is a first value, and substitutes a second output value for the set of data bits if the control signal is a second value.

Heys does not teach providing a different substitution depending upon a value of a control signal. Heys does not teach that the selected S-boxes contain multiple substitutions, and does not teach receiving a control signal that determines which of the substitutions to apply.

Because Heys fails to teach substituting a first output value for the set of data bits if the control signal is a first value, and substitutes a second output value for the set of data bits if the control signal is a second value, as specifically claimed by the applicant, the applicant respectfully requests the Examiner's reconsideration of the rejection of claims 14-20 under 35 U.S.C. 102(b) over Heys.

In view of the foregoing, the applicant respectfully requests that the Examiner withdraw the rejections of record, allow all the pending claims, and find the present application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,



Robert M. McDermott, Esq.
Reg. No. 41,508
804-493-0707